



PISS-IoT: Person Identification and Spotting System in an Internet-of-Things Way

Harish Ram Nambiappan
Computer Science and Engineering
University of Texas at Arlington
Arlington, Texas, USA
harishram.nambiappan@mavs.uta.edu

Sajib Datta
Computer Science and Engineering
University of Texas at Arlington
Arlington, Texas, USA
sajib.datta@uta.edu

ABSTRACT

Missing persons has become one of the most serious issues in many countries around the world. It has been a fact to worry not only for those persons who lost their relatives but also for the law and order officials to search them and find them. So with this kind of problem statement in mind we have created a person identification and spotting system using the Internet-of-Things concept. Our system uses android mobile phone cameras and a server system coded with LBPH Facial recognition along with email sending functions. All these components are interconnected through Amazon AWS cloud in an Internet-of-Things fashion. This is a unique, novel, scalable and better approach, when compared to the previous works because instead of focusing on face detection and recognition in just a single device, our system involves interconnection of face detecting cameras with the face recognition and verification system which is running elsewhere. Also, our system includes the automatic email sending component interconnected with the identification system through cloud which has not been performed in any of the previous works. Experiments were conducted in real-time with real subjects at various locations around the university campus and the system worked very well where the average timings measured from the detection of face till notifying the user with the spotted location was within the range of 30 seconds to 1 minute and 40 seconds with an average value of accuracy ranging from 92 to 96 percent.

CCS Concepts

•**Networks** → **Cloud computing**; •**Human-centered computing** → **Smartphones**; **Ubiquitous and mobile computing systems and tools**; •**Information systems** → **Mobile information processing systems**;

Keywords

Internet-of-Things; Cloud Computing; Mobile Computing; Face Recognition; Android Programming

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

PETRA '18, June 26–29, 2018, Corfu, Greece

© 2018 ACM. ISBN 978-1-4503-6390-7/18/06...\$15.00

DOI: <https://doi.org/10.1145/3197768.3197781>

1. INTRODUCTION

Nowadays many people miss some of their close relatives and their kids at certain occasions and the usual scenario will be like complaining to the police or law enforcement authorities and waiting for their information which takes days, months or even years. Though there are many systems which are currently used to find these missing persons, till now most of the persons who have been missing are not found yet. In most of the important places and landscapes they have attached cctv cameras to monitor people but they are constrained only to that particular place at which they are used. And even if the missing person is identified in those places the concerned people who wish to know their whereabouts won't be able to know about this because the system of cctv cameras are only confined to those places and only people who were present in those places would know about it.

There are some person identification system that has been previously proposed as in [13], [8], [5], [14], [10], [4] and [15]. But they have focused only on either face detection or only on spotting persons using biometrics. And most of the works have been tested only on pre-existing image and video datasets and they were not tested on outdoor areas. Other problems regarding these systems are they need various metrics regarding the person to be identified beforehand and are highly dependent on these metrics such as the fingerprints, footprints, speech patterns, clothing, height, iris of the eye etc. Among these metrics several of them can be replicated and can be used to falsify information while using these person identification systems. Also some metrics such as iris can be analysed only at very close distance which may not be suitable for use at various places. Along with the metrics in some papers the identification system requires some sensors to be made available by the person who is to be identified [13]. The problem in such scenario is that without the sensors the person cannot be identified and the requirement of sensors becomes a necessity which all persons cannot have and cannot be used at every places. The most important thing with all the previous works in common is that they cannot be used in all the places or most of the places.

So we have created a identification and spotting system which works in the Internet of Things concept which can be used at various places. This approach is novel and better than the previous works in many aspects. First we have not focused just on person identification using just one device and a system. We have implemented in a different way through an interconnection of various devices that performs

face detection to a face recognition and verification system that runs separately elsewhere in an Internet-of-things concept through cloud which has not been performed in previous works. There is no need to get too many external metrics and inputs like fingerprints, footprints, speech patterns, other details like clothing, height etc beforehand to identify the person. All we need is the face of the person provided by the user while issuing a complaint through the android application. There is also no need for any external sensors to be present with the person to be identified. The system also focuses on communicating with the users who are concerned about the identified location of the person by notifying them through messages even if they are not present at that location and are bit far away. And this system also works by notifying the message to the user even when they are a bit far away from the spotted location of the missing person. This message sending component is also interconnected with the facial verification and recognition system in an Internet-of-things concept through cloud which has not been done in the previous works. Along with these we have also designed this system not just to work only on pre-existing image and video datasets but we have made it to work on real-life scenario by bringing in subjects and executing the system at various private and public locations such as apartments and department buildings around our university campus and we have obtained very good results even while working with the system in outdoor areas which has not been performed in previous above mentioned works.

Our person identification and spotting system consists of three main components which are interconnected with each other - an android application designed for the user to enter the information and photo of the missing person as a complaint which gets stored in the cloud, android phone mobile cameras which are attached at places acting as cctv cameras which detects faces and takes images which gets stored in a separate cloud and a separate server system which runs facial recognition on the images from those cameras with the missing person images and sends notification mail to the user if there was a match along with the location where the missing person was spotted.

The following section of the paper are organized as follows. In section 2 we have stated the related work done in person identification system as a whole, facial recognition and Internet-of-Things. In section 3 and 4 we have explained in general about facial recognition and internet of things respectively. Also we have explained in detail regarding the concepts that are being used in this paper. In section 5 we have described and explained the system architecture which was created and used for this paper. In section 6 we have explained in detail how we have experimented the system at various locations. In section 7 we have explained the results that were obtained from the experiments. In section 8 and 9 we have discussed the future work that can be done on this system and the conclusion regarding this paper respectively.

2. RELATED WORK

Research has been done and it is still taking place in the field of both face detection and recognition as well as Internet-of-Things. Since the system which we developed consists of separate components interconnected to each other let's see the related work in each of the components.

Now there were also some works that has been previously done on building a person identification system as a whole

which we will explain you now. One of the works involves performing person identification using cctv (closed-circuit television) cameras along with accelerometer and magnetometer sensors within the mobile phones of the persons who are to be identified [13]. Some of the other works focuses on person identification using biometrics of a person which can be either single biometrics or multiple biometrics of a person [8][5][14][10]. Other works include person identification using face detection and recognition in video datasets where speech pattern of a person is also used for identification [4][15].

When it comes to facial recognition though there are many researches going on around, with respect to using facial recognition for identifying specific persons there are some related research works that have been taking place. Research has been performed on person identification by detecting Iris using multiclass SVM [6]. Also dccn-based (Deep Convolutional Neural Networks) face recognition algorithm was used to perform multi-person identification [3].

With respect to Internet-of-Things, various researches have been taking place by considering certain aspects within the field. For example, some researches focus on using Internet-of-Things for a variety of other scenarios while some other works focus on improving the security and privacy while being part of the Internet-of-Things scenario. One of the scenarios involves using Internet-of-things for tracking navigation pattern of birds in an energy efficient manner [1]. Whereas in security scenario, some researchers have focused on privacy and security in Internet-of-Things, focusing on vehicular ad-hoc networks as a medium of connectivity and cloud as a way of authentication for communication between vehicles [2].

Even there are some studies in which authors have focused on using mobile smart phones for various other activities. Researchers have used smart phones as a way of securing their house by making use of the accelerometer and magnetometer in smart phones and detecting break-ins in house [7].

While comparing to the previous studies and researches we have performed many distinctive works in this system. As on considering the person identification as a whole our main focus was not only on facial detection and recognition part or on just Internet-of-Things part. We focused on combining facial recognition with the interconnection of various devices through Internet-of-things concept. And we also focused on the part of establishing communication and notifying the user who are concerned with the identification and spotting of the various persons which was not focused on any of our previous related papers and works. With respect to facial recognition we have used the Local Binary Patterns based face recognition instead of any neural networks or SVMs (Support Vector Machine). We have focused only on the frontal face of a person but we have taken all the features in the frontal face instead of focusing only on certain parts of frontal face. While during experimentation instead of focusing on the static fixed position of the person we detected faces even when the person was moving. In the context of Internet-of-Things we have used the cloud entirely for communication and interconnection between devices without depending on any other communicating networks. Also we have used the cloud for storing user-data and facial images recorded from the phone cameras and for authentication purpose we have stored the ip address of the

phone camera which are used for facial detection and as a part of this system in the cloud. We are also storing the location of the mobile phone cameras with the ip address in the cloud for locating the place instead of depending on GPS (Global Positioning System) and GSM (Global System for Mobile Communications) Networks for spotting location. Also along with this we have been using android mobile phones both for user application and also as a spying camera for detecting faces of missing people when they are in motion by fixing at various locations, without the use of any sensors. So our approach provides a very cost effective solution.

3. FACIAL RECOGNITION

Nowadays various works and research has been done in facial recognition systems. Some research are done to speed up time taken for processing and some are focused on accuracy of finding the person in the images and so on. But the most primary focus of all the facial recognition system is the same - to be able to identify persons in a source (either video or image) with the given list of available faces. Though various algorithms for facial recognition has been created and still many research are going on, it is still not yet used with full effectiveness when it comes to real-time scenario. Among them the most important scenario where it needs to be put to great use is to find persons among the crowd at public places in real-time[12]. In [3] the authors have implemented the testing of their face recognition algorithm in a real-time single classroom environment with students seated in the classroom.

For this paper, we have used the facial detection and recognition using Local Binary Patterns so it is necessary to give a brief explanation on it. Local Binary Patterns is a form of visual descriptor that labels the pixels of an image by thresholding the neighborhood of each pixel and considers the result as a binary number that is either 0 or 1. In the context of facial description the image of the face is divided into several blocks and the Local Binary Pattern values from each block are extracted and concatenated into a histogram. Because of this reason the facial recognition using Local Binary Patterns is also known as Local Binary Patterns Histogram (LBPH)[9]. The reason we have used this method of facial recognition is that it can also be used on images which has lighting variations. In this paper, we will be using LBPH Face Recognition only on frontal face of persons using Python and OpenCV.

4. INTERNET OF THINGS

As we know, Internet-of-Things refers to the interconnection of devices by various means of connectivity through which data is exchanged. There are various ways these devices can be connected. In [1] the authors have used cloud storage and GSM Network through which devices are interconnected and data is shared. Nowadays this concept has been used in various fields and even researches are going on based on improving the security, preserving privacy and reducing traffic while using it. For example in [11] the authors have explained how ad-hoc networks are used in Internet of Things and in [2] those authors have focused their work on using Vehicular Ad-Hoc Networks for communication, security and privacy improvement purposes by using cloud infrastructure.

For the person identification system in this paper the concept of Internet-of-Things is used at two areas - (1) android mobile phone cameras, which is used for face detection, is connected with the server system which runs the facial recognition and sends messages and (2) server system is connected with the user's mobile phones who issued complaint for their missing persons. In the first case both the phone cameras and server system are connected through cloud storage whereas in the second case both the user's phone and the server system are connected through Wi-Fi connectivity for sending e-mails.

5. SYSTEM ARCHITECTURE

Figure 1 shows the system architecture that we have designed and implemented for the person identification and spotting system. The user will enter the information about the person who they have lost along with the photo of that person in their android mobile application which was specifically designed for getting user data. The information obtained from the user data is sent to cloud 1. The photo of the missing person is sent to cloud 2 which is implemented through Amazon S3 whereas the information regarding the missing person is stored in a cloud database implemented through Amazon DynamoDB. The cloud 1 also contains a separate database of ip address of the phone cameras along with the location where they are attached at various places around the university campus.

The mobile smartphone cameras fixed at locations sends images of the persons whose face was detected to cloud 2 that is stored in Amazon S3. But it gets stored in a separate surveillance list inside the storage. The Identification system extracts the images from both the surveillance list and missing person list which then runs the facial verification process. If there is a match with any of the missing person the system then takes the ip address of the mobile phone camera from which the image was taken and checks with the ip address database and finds the location. After this the system notifies the user, who made the complaint with the location where the person was spotted along with time, through email. The email which is sent to the user regarding the missing person location is completely auto-generated based on the information about the person along with the location and time at which the person was spotted.

6. EXPERIMENTATION

Fifteen participants (6 females, 9 males) from our university were used for the experimentation of this system which was held at various places for a certain set of participants. All the participants were aged between 21 and 30 years. Of all these participants 5 were Americans and 10 were Asians. Experiments were conducted at 5 different locations around the university campus: Meadow Run Apartments, University Village Apartments, Engineering Research Building, Nedderman Hall and Centennial Court Apartments. Among these locations Meadow Run Apartments and University Village Apartments were located on the western side of the university campus at Summit Dr and Greek Row Dr respectively, Engineering Research Building and Nedderman Hall were located on the center of the campus at UTA Blvd and Yales Street respectively while Centennial Court Apartments is located on the Southern side of the campus at West Mitchell Circle. In Centennial Court Apartments we con-

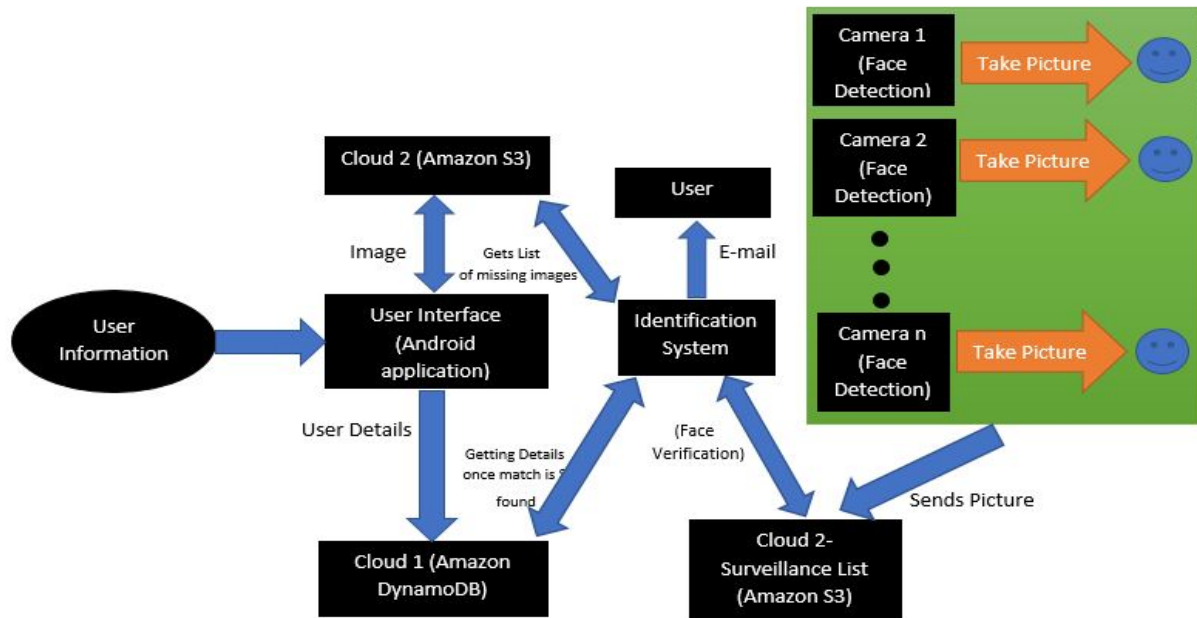


Figure 1: System architecture of the person identification and spotting system used for the experiment

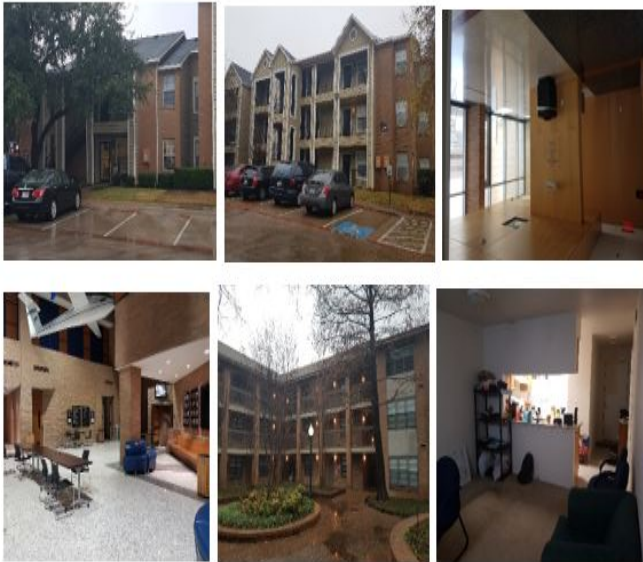


Figure 2: Locations where experimentation and testing of the person identification and spotting system took place (Clockwise from top left) (I) Centennial Court Building 10 (II) Centennial Court Building 11 (III) A public space in Engineering Research Building (IV) Living Room of one of the participants in Meadow Run Apartments (V) University Village Apartments (VI) Nedderman Hall Atrium

ducted the experiments at two different buildings that is Building 10 and 11 located at two extreme ends. In the apartments the cameras were placed inside the rooms of some of the participants. The locations where the exper-

iments were conducted can be seen in Figure 2. Of all these locations, experiments in Engineering Research Building was conducted in day and the experiments in other places were conducted in night, under the lighting of those respective places.

6.1 Devices



Figure 3: Camera attached to the wall at various locations for testing

For the experimentation of this system we have used camera in the android mobile phones and a laptop performing as the server system which runs the facial recognition and email sending functionalities. The android mobile phones were of Android version 7.0, with a camera taking pictures of 16:9

aspect ratio, and the system with the facial recognition and email sending functions was a Dell Inspiron 15 7000 Series Laptop which uses Windows 10 64-bit Operating System, with Intel Core i5 x64-based processor along with a 8 GB RAM, and the code was built on Python which runs on Py-Charm IDE. The version of python is Python 3.5.4. Libraries in Python such as opencv for facial recognition and boto3 for connection to Amazon AWS services were used in the system code. As shown in figure 3, phone camera were attached at the walls in various locations where we conducted the experiments.

6.2 Experiment Methodology

During the experiments for the system we made the participants move around the place and make them pass through the mobile phone camera. Since we were focusing only on the frontal face the participants were requested to show their entire front face in front of the camera and then move out from the front of the attached mobile phones. The distance between the camera and the participants varies depending upon their height. Based on their height, the participants were told to position themselves while moving in front of the camera so that their face will appear on the camera and can be detected. For some person we also took the readings while they were wearing eyeglasses and also when they removed their eyeglasses. As shown in Figure 4 the participants were made to move in front of the mobile phone camera and were made to show the front face to the phone camera and then move out from the front of the camera. We were measuring the speed as well as the accuracy of the system. The speed was calculated by measuring the timing from the camera starting to detect the face of the person till the system sending the email to the user when there was match found with respect to that person.

7. RESULTS

Figure 5 shows the email that has been automatically generated by the system in order to notify the users who issued the complaint regarding the missing person. As you can see in Table 1 the overall speed, which was measured through the timings, was within the range of 30 seconds to 1 minute and 40 seconds which is really very fast. And also with just focusing on the frontal position of the face without changing any orientation we were able to get accuracy within the range of 92 to 96 percent. Since while moving in front of the camera, the system detects the face multiple times so when each time the face is detected the face verification process is performed. As a result, the accuracy is calculated by comparing the number of times the face is correctly verified with the number of times the face is detected for each person. Places like Nedderman Hall, Meadow Run Apartments and Engineering Research Building, where lighting conditions were very good, showed a high accuracy rate when compared to the other places which had moderate to good lighting conditions. Figure 6 and Figure 7 shows the graphical representation of the average speed and average accuracy of this system obtained through testing at various locations.

You can also see that at places like Centennial Court Apartments Building 10, Nedderman Hall and Engineering Research Building the timings were a bit high. The reason was because of the slow speed of the Wi-Fi connection at Centennial Court Apartments Building 10 and Wi-Fi network traffic in Nedderman Hall, Engineering Research

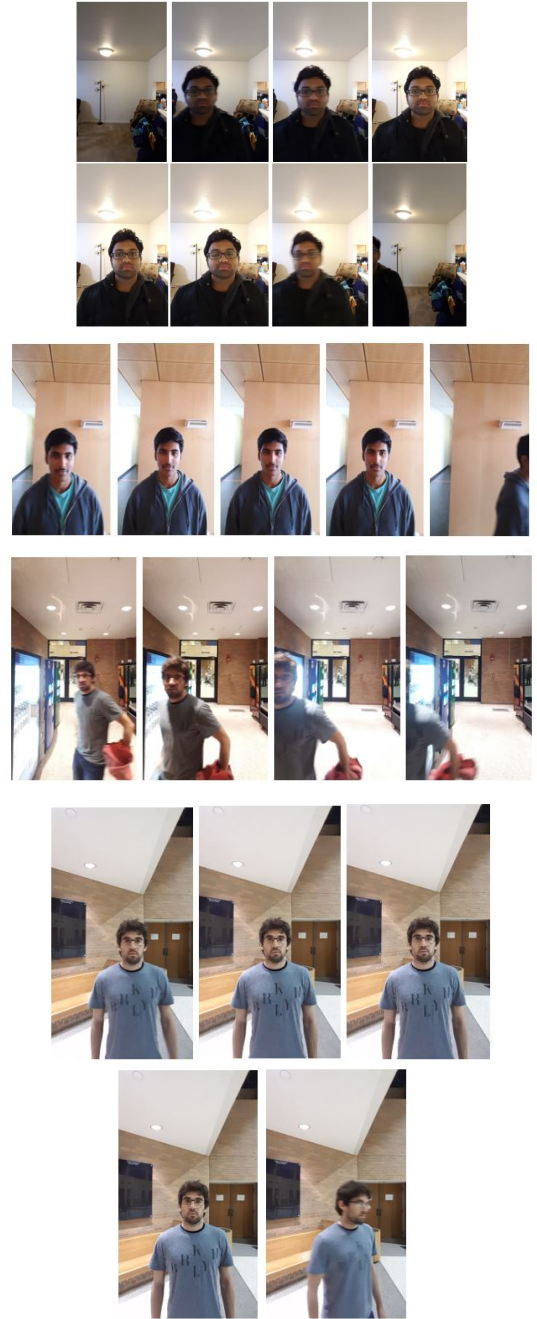


Figure 4: Faces detected while the people are moving in front of the camera at experiments conducted in various locations namely (From top to bottom) (I) Meadow Run Apartments (II) Engineering Research Building and (III and IV) Nedderman Hall in real-time

Building both being public places with lots of student crowd. And also the time taken for recognizing the person without eyeglasses was less than the time taken for recognizing the person with eyeglasses at locations where it was tested. The reason probably lies in the process of Local Binary Patterns where the facial image is divided into regions to obtain the



Figure 5: The email used to notify the user who issued the complaint about the missing person that has been auto generated by the system based on the information about the name, location where the missing person was spotted along with the time when the person was spotted

LBP descriptors from each region of the image [9]. Since the image is converted to grayscale before processing, to avoid the illumination issues, the LBP descriptors obtained from the region of the face where the person is wearing eyeglasses must have been similar in various images. As a result, when the LBP descriptors from all the regions are concatenated to form a global description of the face there must have been some mismatches while verifying the surveillance images with that of the image of missing persons.

The overall average accuracy of our person identification system through the values obtained from all the locations is 93.75 percent. Figure 8 shows the comparison of our overall average accuracy with the overall accuracy values as stated in [4], [14] and [8]. Note that the accuracy values stated in those papers are obtained either by performing experiments on pre-existing datasets or by creating an experimental setup in just a single particular location. But after performing experiments on various locations around the campus and by making the subjects moving in front of the camera in real-time environment our person identification system has been performing very well when compared to the other systems shown in Figure 8.

Table 1: Results obtained from the experiments that was conducted at various locations around the university campus

Serial No	Location	Average Speed	Average Accuracy(in percentage)
1	Meadow Run Apartments	31.90s	96
2	University Village Apartments	30.37s	92
3	Centennial Court Apartments Building 11	39.28s	92
4	Centennial Court Apartments Building 10	1m 19s	94
5	Nedderman Hall (while wearing eyeglasses)	1m 40s	93
6	Nedderman Hall (without wearing eyeglasses)	51.25s	94
7	Engineering Research Building (while wearing eyeglasses)	46.21s	94
8	Engineering Research Building (without wearing eyeglasses)	45.09s	95

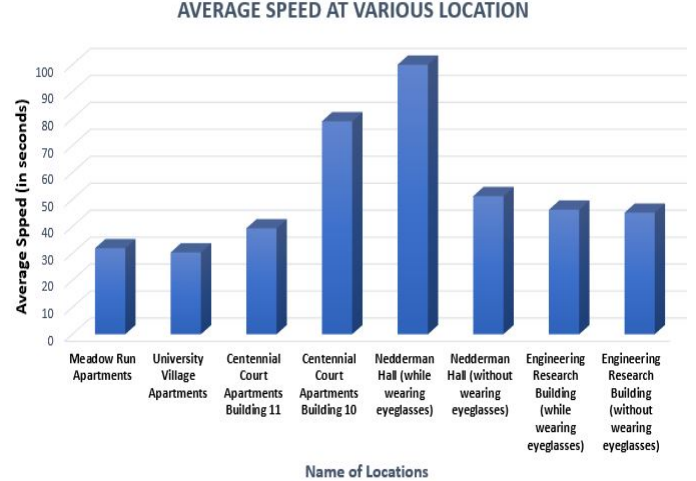


Figure 6: Graphical Representation of the Average Speed of the Person Identification System obtained through testing at various locations

8. CONCLUSION

We have developed a person identification and spotting system using the Internet-of-Things concept by interconnecting devices such as android mobile phones and their cameras along with a server system which will be running the facial recognition on frontal face position of the faces of the detected persons and sends email to the concerned per-

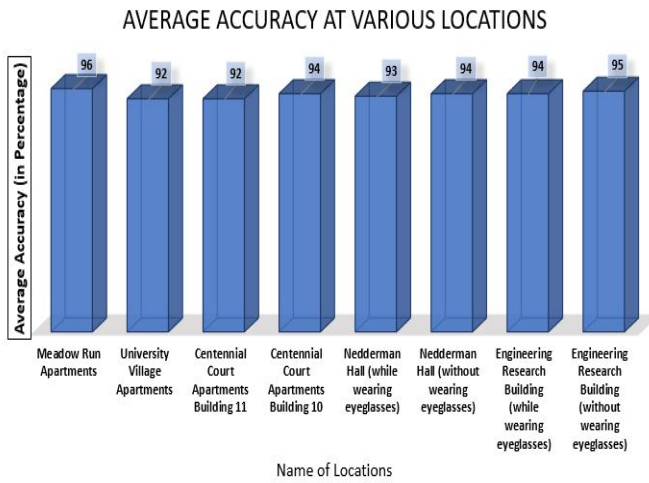


Figure 7: Graphical Representation of the Average Accuracy of the Person Identification System obtained through testing at various locations

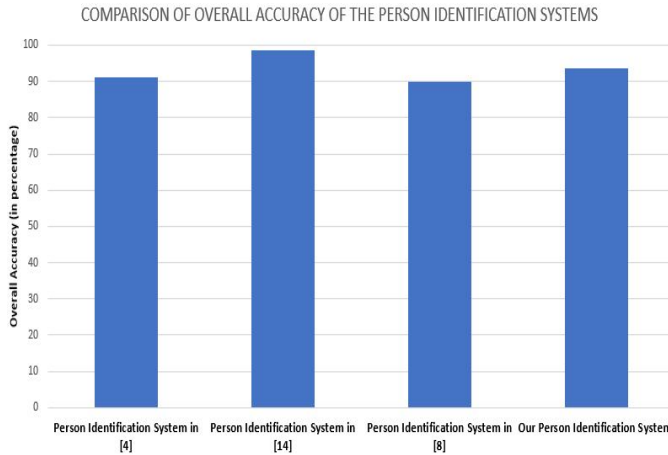


Figure 8: Comparison of the average accuracy value obtained from our person identification system with the overall accuracy values stated in [4], [14], [8]

sons once a match is found. When compared to the previous works this is a unique and novel approach which focuses on detecting and identifying the person as well as focuses on notifying the users who are in need to know the location of the person even when they are far away. It is a cost effective solution as it utilizes old and used android mobile phone cameras for face detection. It is also a scalable and comprehensive solution than the previous works because it incorporates interconnection of face detecting cameras with the server system along with the email sending component which is also connected to the system. The system has also been tested with real-life subjects in real-time at various outdoor areas around the university campus which has not been done in previous works. The system was tested at various locations around the university campus which includes apartments and public halls. So far the system has been working really well with the timings falling within 2 minutes for detecting the person and notifying the concerned

users along with the accuracy rating with the range of 92 to 96 percentage which is a highly desirable outcome.

9. FUTURE WORK

There is a room for various improvements that can be done on this system in the future. Especially planning is to be done in improving the security of the system. Also some work needs to be done in implementing the system by replacing the android mobile smartphone cameras with either cctv cameras or ip cameras because the android phone cameras are fixed to a static position and can't rotate to view at other angles. Instead of depending on just the frontal face certain work needs to be done to also recognize the faces even when the face is turned at various different angles by using an improvised face recognition algorithm or by creating a new face recognition algorithm. The system requires additional functionality and testing such that it also works when there are multiple faces of various persons detected at the same time. Even for the mobile application for giving complaints about missing person some work needs to be done on making it compatible with iOS devices such as iphones, ipads too.

10. REFERENCES

- [1] C. Alippi, R. Ambrosini, V. Longoni, D. Cogliati, and M. Roveri. A lightweight and energy-efficient internet-of-birds tracking system. In *Pervasive Computing and Communications (PerCom), 2017 IEEE International Conference on*, pages 160–169. IEEE, 2017.
- [2] W. Jiang, F. Li, D. Lin, and E. Bertino. No one can track you: Randomized authentication in vehicular ad-hoc networks. In *Pervasive Computing and Communications (PerCom), 2017 IEEE International Conference on*, pages 197–206. IEEE, 2017.
- [3] J. Kim, S.-S. Yun, B.-N. Kang, D. Kim, and J. Choi. Reliable multi-person identification using dcnn-based face recognition algorithm and scale-ratio method. In *Ubiquitous Robots and Ambient Intelligence (URAI), 2017 14th International Conference on*, pages 97–101. IEEE, 2017.
- [4] S. Kokila and B. Yogameena. Face recognition based person specific identification for video surveillance applications. In *Proceedings of the Third International Symposium on Women in Computing and Informatics*, pages 143–148. ACM, 2015.
- [5] R. Kushwaha, N. Nain, and S. K. Gupta. Person identification on the basis of footprint geometry. In *Signal-Image Technology & Internet-Based Systems (SITIS), 2016 12th International Conference on*, pages 164–171. IEEE, 2016.
- [6] R. Luhadiya and A. Khedkar. Iris detection for person identification using multiclass svm. In *Advances in Electronics, Communication and Computer Technology (ICAECCT), 2016 IEEE International Conference on*, pages 387–392. IEEE, 2016.
- [7] M. A. Mahler, Q. Li, and A. Li. Securehouse: A home security system based on smartphone sensors. In *Pervasive Computing and Communications (PerCom), 2017 IEEE International Conference on*, pages 11–20. IEEE, 2017.

- [8] E. Martinson, W. Lawson, and G. Trafton. Identifying people with soft-biometrics at fleet week. In *Proceedings of the 8th ACM/IEEE international conference on Human-robot interaction*, pages 49–56. IEEE Press, 2013.
- [9] M. PietikÄäinen. Local Binary Patterns. *Scholarpedia*, 5(3):9775, 2010. revision #183551.
- [10] C. V. R. Reddy, K. V. K. Kishore, U. S. Reddy, and M. Suneetha. Person identification system using feature level fusion of multi-biometrics. In *2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, pages 1–6, Dec 2016.
- [11] D. G. Reina, S. L. Toral, F. Barrero, N. Bessis, and E. Asimakopoulou. *The Role of Ad Hoc Networks in the Internet of Things: A Case Scenario for Smart Environments*, pages 89–113. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.
- [12] L. Rothkrantz. Person identification by smart cameras. In *Smart City Symposium Prague (SCSP), 2017*, pages 1–6. IEEE, 2017.
- [13] T. Teixeira, D. Jung, and A. Savvides. Tasking networked cctv cameras and mobile phones to identify and localize multiple people. In *Proceedings of the 12th ACM international conference on Ubiquitous computing*, pages 213–222. ACM, 2010.
- [14] S. Verma and C. Singh. Efficient person identification from periocular region using intelligent fusion of local and global features. In *2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pages 1–5. IEEE, 2017.
- [15] Z. Xiong, Y. Chen, R. Wang, and T. S. Huang. Improved information maximization based face and facial feature detection from real-time video and application in a multi-modal person identification system. In *Multimodal Interfaces, 2002. Proceedings. Fourth IEEE International Conference on*, pages 511–516. IEEE, 2002.